HAKIN9 ON DEMAND

Vol.3 No.2
Issue 02/2014(17) ISSN: 1733-7186

CERTIFIED ETHICAL HACKING IN A NUTSHELL

ALL-IN-ONE COMPENDIUM TO GET YOUR CERTIFICATE

WHY AND HOW TO BECOME AN ETHICAL HACKER? GENERAL FIRST STEP

WHAT IT MEANS TO BE A HACKER?

HOW TO START ARRIER AS CERTIFIE HACKER

ONLY IN HAKIN9 MA

WHAT HAPPENED WIT COUNCIL WEBSITE IN FEBRU

Dr.Web 9.0

for Windows — the rapid response anti-virus

1. Reliable protection against the threats of tomorrow
2. Reliable protection against data loss
3. Secure communication, data transfer and Internet search

www.drweb.com

Free 30-day trial: https://download.drweb.com

New features in Dr.Web 9.0 for Windows: http://products.drweb.com/9

FREE bonus — Dr.Web Mobile Security:
https://download.drweb.com/android

Developing for Amazon Web Services?

Attend Cloud DevCon!

Cloud DevCon

June 23-25, 2014
San Francisco
Hyatt Regency Burlingame

www.CloudDevCon.net

Attend Cloud DevCon to get practical training in AWS technologies

- Develop and deploy applications to Amazon's cloud
- Master AWS services such as Management Console, Elastic Beanstalk, OpsWorks, CloudFormation and more!
- Learn how to integrate technologies and languages to leverage the cost savings of cloud computing with the systems you already have
- Take your AWS knowledge to the next level – choose from **more than 55 tutorials and classes,** and put together your own custom program!
- Improve your own skills and your marketability as an AWS expert
- Discover HOW to better leverage AWS to help your organization today

Register Early and SAVE!

A BZ Media Event

CloudDevCon

Certified Ethical Hacking in a Nutshell

Table of Contents

Dear Readers,

This is a special issue, which describes a Certified Ethical Hacking training and certificate, provided by the International Council of E-Commerce Consultants (EC-Council).

Ethical Hackers are employed by company to do a penetration test of their systems, using the similar methods and tools as hackers have; it allows to know the weak points and vulnerabilities in security.

More details in text of our Authors, who describes what do you gain and what are the possibilities when you are a CEH. And they are numerous – you can read about it in three texts! But there is one thing which appears in every article – you have to keep learning, improving your skills. The passing the CEH training is just a begin. Even when you are a Master of Security, you have to keep developing your skills and knowledge. Why? You can find the answer in special article of Hakin9 Magazine team – a story of hack attack on EC-Council website.

Then, apart if you are CEH or you are just considering the training, and even if you doesn't – it is worth to read the article of Mr. Darko Mihajlovski and meet the actual hacking techniques in industrial environment. Start learning just now!

Hakin9 Magazine Team

Editor in Chief: Ewa Duranc
ewa.duranc@hakin9.org

Managing Editor: Michael Rogaczewski
rogaczewski.michal@hakin9.org

Betatesters & Proofreaders: Aidan C., Phil Patrick, Elia Pinto, Kishore PV, Hani Ragab

Special thanks to our Beta testers and Proofreaders who helped us with this issue. Our magazine would not exist without your assistance and expertise.

Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

Product Manager: Ewa Duranc
ewa.duranc@hakin9.org

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Art. Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@hakin9.org
DTP: Ireneusz Pogroszewski

Marketing Director: Ewa Duranc
ewa.duranc@hakin9.org

Publisher: Hakin9 Media sp. z o.o. SK
02-676 Warszawa, ul. Postępu 17D
NIP 95123253396
www.hakin9.org/en

What it Means to be a Hacker?

by Chrissa Constantine

The more I looked the more questions arose. What is a hacker? Who hacks? Are they young or old? Why do they hack? Are they criminals or heroes? The more I researched the more I realized that there is no one answer. This is the journey to discovery.

The mystery and anonymity encompassing hacking and the various personae assumed in the cyber world make it challenging to identify individual motivations. My investigation evokes a movie quote, “Well, opinions are like assholes, honey. Everybody’s got one and everybody thinks everybody else’s stinks”. When it comes to defining hacker ethics, motivations and profiles, there are plenty of opinions and theories.

Data from past documented cases on hacking, an array of articles on hackers who were caught, and online questionnaires and profiles have yielded abundant theories about how to profile criminal hacking activity and how to understand motivations behind computer hacking.

Evidence left after a hack and profiles obtained from documented cases have also provided a means to explore the characteristics of hackers and to explore differences and similarities in the hacker culture, but there does not appear to be one single means to perform an accurate profile for a hacker. Just as there is an array of perspectives on motivations, there is incredible controversy over the word “hacker”, and the social and ethical perspectives of hacking are still extensively debated.

Let’s explore the evolution of the word “hack” and “hacker”. The word “hack” and its definition has changed, and now this term is used to describe people in sociology, psychology, neurology, and art. For example, social engineering is described as “human hacking”. Social engineering uses human and technology-based techniques to obtain desired information. This essay does not attempt to cover social engineering, however, Chris Hadnagy has developed a social engineering framework and pioneered the usage of the phrase “human hacking”. In contrast, a “computer hacker” is addicted to computers and technology and is capable of discovering a creative or innovative resolution to problems involving technology. Examination of the language and slang can provide a window into how hackers view the world. There are several artifacts on the Internet that provide insights such as The Jargon File, located here: *http://www.catb.org/jargon/html/index.html*.

In the 1960s, the term “hacking” had a positive connotation, and it was during this time that the name entered computer culture at Massachusetts Institute of Technology. A change in meaning of this word occurs in the late 1980s and early 1990s, and what used to be a positive or even flattering appellation became affiliated with cyber crime.

In order to find out when the word started gaining in popularity I analyzed Google Trends charts, between the years 2008 and 2014, which show a significant increase in journalistic reporting on hacking and cyber crime, particularly in the U.S, UK and India. Yet disagreement exists over modern meanings of the term of a criminal and the initial meaning of a creative programmer. Interpretations encompass everything from creative people who are self-motivated and love learning about technology to criminals who use computers for illicit purposes. To me, the word “hack” is subtly nuanced and hackers can be considered individuals who are ingenious and creative.

Where the word “hacker” has variants, so too does the word “hack”. Hack has two definitions and one meaning could be considered offensive. When hack is used as a noun, it signifies someone who produces unoriginal or substandard work. Alternatively, hack can likewise refer to an ingenious resolution to a problem. Likewise, in the media, the term implies stealing and within the hacker community it implies creating. Within the hacker community, it was in the second half of the eighties that the terms “hacker” and “hacking” started to change in meaning.

When it comes to words, hacker culture is a loosely networked group of subcultures that have it’s own language, jokes, values, stories, heroes and scoundrels. Hackers relish wordplay, and among hackers slang delivers a variety of shared meaning and encodes the nuances of a spectrum of mental states and problem-solving

that transcend conventional linguistic rules. In other words, hackers are very deliberate and inventive in their usage of terms and language, and much of the time verbal wit is employed as a competition or test.

An examination of the generations of hackers from 1960 to the current time illustrates shifting perceptions. Hackers were known for technological curiosity and were accepted for their contributions to the computer industry, over time this attitude shifted, and there has been an increase in malicious computer hacking. The acceptable bounds of technical exploration have become hotly contested. There is a clash between those seeking to maintain the original hacker ethos and those striving to create new values for the ubiquitous dissemination of computers and technology in our lives.

Currently, media refer to cyber criminals as “hackers”, but the original term did not have a negative connotation. Originally the word “hacker” referred to someone who was innovative and could figure out unique ways to solve issues. In 2014, there are many individuals who call themselves hackers who do not have a computer science or programming backgrounds. Some are actually novices who are able to use tools that are readily available on the Internet. Some tools are free, and other tools are available for a fee making it possible for an unskilled criminal to use a computer to commit a crime. The level and complexity of attacks appears to be increasing, but the actual skill set of the cyber criminal appears to be decreasing due to the use of automated tools that are widely available.

The computer underground yields a mix of real-world relationships and the digital immateriality of cyberspace, where boundaries blend and relationships are dynamic. The intersection of “real-world” and the digital-world result in a loose affiliation of social ties and for some hackers, a perception that the two are one world.

Groups are not coherent, and the boundaries between them are fluid, resulting in difficulty in identifying what constitutes a member within various hacking communities. Another aspect that makes research challenging is the climate of secrecy and fear or suspicion that arises due to the legal implications of hacking. Secrecy and anonymity make it difficult to obtain accurate information about motivations and characteristics of hackers.

Generations of Hackers and Motivations

Why hack? What are the motivations behind hacking? Hacking motives range from intellectual curiosity and discovery to political reasons or money, and this article attempts to reveal some of the primary motivations of hackers from the 1970s to 2014.

Researchers and journalists have provided accounts of a hacker’s motivations and surveys and interviews have provided hacker profiles. One group, the Hackers Profiling Project (HPP), has applied criminal profiling to hackers, and uses an online survey in an attempt to obtain motivations for hacking. Many studies rely upon the subject’s own classification and motives for hacking, which may result in biased information. Other theories are derived from psychology- and sociology –based theories of crime, and were applied to hackers in an attempt to describe motivations behind criminal hacking activities.

I define time periods as a means to group hackers and to show how behavior and ethics behind hacking activities evolve. I want to note that not all hackers are criminals and that this is an attempt to identify basic trends and perhaps provide perspective on the many facets of hacker culture. Many motives for computer hacking have been proposed such as curiosity, peer recognition, desire for power, self-esteem or financial. I hope the timeline provides an understanding of how most hackers embraced a particular ethos until now where there are many splinter groups and rationales behind why an individual hacks computers.

As early as 1878, there are recorded examples of technological mischief. This was when switchboard operators hired by phone companies intentionally misdirected or disconnected phone calls, eavesdropped or played pranks on customers. During the 1930s, cryptologists intercepted messages and broke the Enigma code. Even Richard Feynman picked locks and played jokes on colleagues during his time at Los Alamos. “After I was able to open the filing cabinets by picking the locks, they got filing cabinets that had safe combinations. Now, one of my diseases, one of my things in life, is that anything that is secret I try to undo. And so the locks to those filing cabinets represented a challenge to me”, Feynman wrote, “So I always figured they were keeping the method a secret, and like a kind of disease, I kept working on these things until I found out a few things”. This early obsession with working on things until discovering a secret is

similar to motivations from hackers that span multiple generations. Hacking is an obsession and figuring things out is imperative.

What I call the "first generation" of hackers falls between the 60s and 70s, and begins with university students from MIT at a time when computers were rare. The beginnings of the hacker culture emerge at MIT when the Signals and Power committee of MIT's Tech Model Railroad Club started inventing tools, slang and a culture around technology. There is also a fun website for MIT that is dedicated to hacks: *http://hacks.mit.edu/Hacks/*.

In the 1970s hackers known as "phreakers" were exploring phone systems. These hackers discovered and exploited the characteristics of the telephone-switching network. In 1971, blue box phone "phreaking" is first reported in Esquire Magazine and in an article by the Los Angeles Times. Phreakers could be considered an early example of the anti-establishment subculture within the larger hacking community. This is the time when intelligent people were exploring and contributing on a technological level. This time could be considered a renaissance of the hacker culture.

Programmers during the 1960s and 1970s had much in common with artists because they were making software for computers, which is another form of creative expression. In 1966, Bell Labs engineer Billy Klüver and artist Robert Rauschenberg collaborated in a group that experimented with using art and technology. There were many endeavors during that time to bring artists and engineers together, and there was incredible innovation in using computers for art, music and animation.

In 1960-1970s, the first generation of hackers had a desire to explore and visit new worlds by conquering technology and the issues that it presented. Many individuals who started hacking during this time were addicted to discovering how computer networks, systems and technology worked. They desired a deep understanding of all aspects of computer systems or technology.

Yet others during this time wanted to learn more about computer security and were driven to understand the underlying principles and to share what they learned. Often the individuals in this time frame worked or hacked alone but would share their knowledge within a group. This generation had a strong hacking ethic. There is much information regarding the hacker ethic, but suffice it to say that digital explorers during this time were programming enthusiasts who wanted to modify programs to customize or optimize them or to just to have fun learning how things worked.

In the late 1970s to early 1980s, exploration of computers, phone systems and other technology were not typically destructive. Often exploits were considered playful excursions. In the 1980s, the introduction of "personal" computers created a turning point in hacking history. During this time computers were no longer limited to business users or hobbyists – anyone could have one for their own purposes. During the early to mid-1980s, the Internet protocol suite was standardized, and access from personal computers were connected through modems and telephone lines, which ushered in a new age of personal computing.

In 1984, Steven Levy wrote a book detailing hacking history and exploring their values and belief system, which he termed the "hacker ethic". The hacker credo can be summarized as, "Access to computers, and anything that might teach you something about the way the world works, should be unlimited and total". While much has been written about hacker ethics, it is unclear how many hackers actually subscribe to them, and for those that do to what extent they adhere to those principles. Essentially, Levy's work reflects a hacker attitude that rejects hierarchy and authority, promotes decentralization and an attitude of information sharing. These attitudes can be seen even in hackers today.

By the late 1980s, the hacking community starts to divide, and a number of hackers are no longer satisfied with exploring systems for fun or just to see how they work. The divide came when some hackers sought to direct their knowledge toward criminal intent, including pirating software and games, and creating viruses and worms. This group splintered even further into groups that hacked to obtain sensitive information from governments, research facilities, or large corporations. Not long after that these rival groups start fighting each other.

For hackers in this divided group from the 1980s, there was often attention seeking and ego-driven behavior motivating their hacking. During 1989, hackers started to use computers as a tool to debate political issues, which lead to a new term. In 1996, the term "hacktivism" was coined by Omega, a member of the Cult of

the Dead Cow. A hacktivist may not be focused on just one political party. Often hacks include website defacement and may be a response to political disorder, unrest, or even a court decision. Motivations for hacktivism tend not to be profit driven. Hacktivism may lead to using tactics to embarrass the individual or organizations in question. The term for this is called “Doxing”.

These darker forms of hacking satisfy three objectives with varying degrees of harm. One objective is to attempt to gain unauthorized access to a system to satisfy personal motives such as pride, curiosity or to feed the ego. The second seeks to gain unauthorized access to tamper with or to destroy information. The third seeks to gain unauthorized access to systems to steal data for criminal purposes. The systems under attack are typically research institutions, university, government agencies or large corporation or public utilities. Most of the hackers in this category are involved in corporate or government espionage and have connections to organized crime.

In the late 1990s, a third generation of hackers emerged who wanted to be remembered for their contributions. Others wanted to create improvements or increase computer security. Motivated by exploration and fun, systems would be hacked. Sometimes system owners would be shown how to fix the issue. Hacker ethics start to change during this time.

During approximately 1994, tools emerge for use by “script kiddies” or individuals lacking coding skills. Script kiddies use pre-built tools to attain their goals because they lack the programming skills, and will download tools from the Internet. These individuals seek opportunities to vandalize or disrupt systems. This attitude and behavior are distinctly different from the earlier generation of hackers who were computer programmers, and who adhered to what could be called the hacker ethic. Earlier generations of hackers championed free sharing of information and did not harm data that was found in their forays.

In 1998, a group of hackers call L0pht coined the term “grey hat” to describe their behavior. This means working without permission, possibly breaking laws to expose computer vulnerabilities. There are two other categories of hacker that have been defined, white and black hat. White hat hackers work with permission and obey the law. Black hat hackers have their own ethical code and have no issues with breaking the law. They can be seen as having no scruples.

Some third generation hackers also hacked for the thrill and spirit of adventure or ownership of systems. The slang term for owning or conquering a system is to “Pown”. This term implies humiliation of a rival. Some may even have had a desire for fame and would feel an adrenaline rush at the challenge of controlling a system. Others pushed the limitations of the systems they hacked, and chose to hack systems seen as invulnerable as a means to have pride over doing something others see as impossible.

A fourth generation emerges in 2000. These individuals hack for reasons that range from boredom to attention getting. Others start to use hacking as a tool to leverage social and political issues. Hacking during this time may be used as a defense against a violation on the online or cyber world. Hacking attempts may even be used as a defense against a situation in the physical world that is deemed morally corrupt.

Many times hackers in this generation have a mission and hate the “system”. They seek change and may even believe they are providing a service because they share access to things they think should be free. They may even see themselves as freedom fighters whom are seeking to correct injustice and who fight for basic human rights. These individuals may believe that the media and the general populace are misinformed about their mission and who they are, which in turn leads to fear and the wrong perspective about their rationale for hacking. These hackers do not consider themselves criminals, but rather view criminals as censoring the information and stopping the truth.

In the late 2000s, there started to be more frequent conflicts with authority. Many times hackers would see the activities of authorities as violating or invading personal privacy. Targets of these professional hackers may be the military, governments, or industrial establishments. These targets are seen as oppressors and may be picked out due to a hackers’ political or ideological motivation. Hacking may be used as a challenge to figures of authority or to feed their ego. The hacker in this category may openly challenge authority and may even feel a sense of gratification in hacking a system run by an “expert”. These hackers desire elite status and derive pride and satisfaction by challenging authorities and bringing themselves to greater heights. Authority may be parents or adults, police, governments, corporations or others that are seen by the hacker as having some form of control or authority.

Security experts from a variety of professions start to emerge on the hacking scene around the year 2000. These security experts are considered hackers and may work for or may have had prior positions with the military, governments or corporations. Espionage or counterespionage in this group may be leveraged to test computer or security vulnerabilities, and these hackers often use smaller organizations to launch attacks against their larger, final targets. In 2010, the first recorded sponsored attacks, which typically the government funded occurred. These professional hackers are motivated by profit alone and may have political or ideological targets or motivations.

In 2014, hacking motivations do not all fall within the law, nor do they fit the earlier hacker ethics. Individuals craving fame and notoriety use hacking as a means to obtain attention. Attention seekers who use hacking do so within a group, and think hacking makes them cool or makes them stand out. Others hack to demonstrate power or to avenge a wrong, and use hacking to wage personal wars. Some may be angry and lack the skills to express their emotions, which lead to hacking due to rage or revenge. Hacking may be used to direct anger or disgust against perceived wrongs or slights. Some are purely motivated by profit or greed, and use hacking as a means to attain personal financial gains. Yet others feel frustrated and use hacking to escape out of control feelings, desires, or situations. Hackers in this category may desire escape from family or society, and seek refuge in computer use or technology. Often they see themselves as misunderstood and as loners. These hackers use hacking skills as a coping mechanism to handle loneliness and isolation.

Criminal Activity

There are no consistent or widely accepted theories or frameworks regarding why or how people become hackers nor is there is clear or effective guidance on what to do to prevent an early interest in computers from evolving into criminal hacking behavior. There are many studies on the technical, sociological, psychological and cultural origins of hacking with various perspectives, but there are quite divergent theories that arise due to differences in theoretical perspective.

In 1999, the FBI made an attempt to profile hackers, and posts defining hacker profiles range from nerds and geeks, to teenage geniuses, to antisocial, psychotic underachievers and loners. Hackers from these profiles are seen as having more technical prowess than ordinary people, but are categorized as weak in other areas such as communication or social skills. There is a database of hackers that apparently rivals the one from the FBI. It is located at SOLDIERX.com and is called the “World’s Largest Public Hacker Database”.

While there are many theories and “profiles” of a hacker, some important generalizations can be made to explain why an individual may develop criminal tendencies as they develop hacking skills. First, there is often a lack of consequences for those who begin hacking at an early age. Second, hacker behavior is reinforced through communities that encourage each other and through media attention that can at times glorify such behavior. Motivational themes have been identified for hacking behavior such as curiosity, compulsion to hack, need to create control or order, attraction to power or fame, peer recognition or belonging to a group.

Computer criminals make an appearance in reports of corporate crime starting in the 1970s. In the 70s, crimes in the United States involved mostly destruction of computers or computing equipment. It took time for cyber crime to become prevalent because criminals did not have computer access, nor did they necessarily possess the expertise to use computers for criminal activities. There were no easy ways to interact with early computing environments. When computers became less expensive to buy and easier to use, cyber crimes increased, which is why the media did not report on cyber crime until the 70s.

The use of computers and technology has increased in our daily lives resulting in more access to tools and means to commit cyber crimes. The use of computer technology for criminal activity is unique because the Internet and the digital world do not have borders and because there is a blurring between what is real and virtual. The advent of the Internet has created a virtual world that could be considered separate from the world in which we live, which may be why some hackers are able to perform criminal acts with computers. Maybe this idea of the virtual world separates it from their psyche and provides an alternative to reality.

The fourth generation of hacker is the largest group to fall into criminal activity, not only because of the ease to obtain tools and technology, but because there are more young people who continue to hack from their teens into their twenties. While there were reports of criminal activity in the 1970s, the motivation behind

hacking was mostly for fun and exploration, and was a deep obsession to figure out secrets or what made things work. Fourth gen hackers are often driven by the desire for notoriety and bragging rights within their peer group. There appears to be a general disregard with fourth gen hackers for the history, culture or ethics of the generations of hackers from the 1970s, 1980s and 1990s.

The fourth generation of hackers is often motivated by profit and may be driven by anger. These cyber criminals want to make money through any means necessary, and steal from consumers and businesses alike. They may attack a small business or consumer or a large enterprise. The most recent example of hacking for profit in the news is the attacks on the credit card industry and on ATMs. There is also a rise in hacktivism and cybercrime. The type of hacker motivated by profit, driven by anger, or acting out political motivations, is quite different from the hacker who hacked to gain understanding, knowledge and skill with technology. Those hackers had a different ethos and were often driven by curiosity or addiction to technology. Some hackers from the first generation were also from troubled homes and used hacking as an escape mechanism.

For adult criminal or deviant behavior that involves hacking one theory defines social development and role of personal character traits as a factor to adults continuing to hack for a criminal purpose. Two primary causes of individuals hacking are that most hackers tend to be young males in their late teens and early twenties who are trying to handle adolescence. This period may be associated with youthful participation in various forms of delinquent or antisocial behavior. The second cause would be a lack of ethical standards or guidelines that would allow young hackers to apply moral principles thereby regulating their own behavior. Many times hackers act upon their impulses with limited regard to the effect of their behavior on others. While this tendency may define behavior during the adolescent stage, the transition to adulthood and related deviant behavior requires more examination.

A couple of clear findings arise regarding what motivates individuals to start hacking. Most hackers develop an interest in computers early in their lives, and the interest appears to develop with mostly innocent motives, which is a drive or curiosity to understand how computers work. It is also apparent that most hackers are exceptionally bright compared to their peers and that most young hackers appear to be uninterested in being a superior student in school, rather they would prefer to spend their time learning to hack or on more interesting things than academics.

Many hackers appear to connect with others of like interests at some point in their hacking history. Hackers and potential hackers seek each other out through online communities and bulletin boards or chat rooms. These individuals form their own communities and significantly develop skills and techniques during this time. During this phase, young or new hackers may seek approval from their peers and this can lead to criminal activity.

New hackers may seek out experienced hackers to act as mentors, and may become more solitary after training with a mentor. Some hackers prefer to work alone possibly due to an increased feeling of security. Groups may provide support in the form of belonging, personal identity development or for sharing responsibility or learning new skills. For hackers that may develop into criminals, an attempt may be made to identify youth that are at risk of becoming a hacker and providing support and intervention.

Many times college age hackers will find jobs in IT or in information security once they finish college. If the hacker did not do well in school and did not get into college, then there is a stronger possibility that person will use hacking skills to do harm. The question here would be if an individual were out of work and needed money to pay for food or rent, would he/she deviate from his/her principles and hack to provide a means to support oneself. Most hackers in this category would answer in the affirmative.

How does Hacking Emerge and who are Hackers?

Several frameworks can be used to apply criminal profiling and used to describe the behavior underlying hacking activities. I am not an expert in psychology or profiling, but some of the following concepts can to further examination of this fascinating topic.

Criminal profiling arose in 1970 when the FBI started a program called Applied Criminology. FBI agents interviewed serial murderers to develop theories and categories of various offenders. Currently, the FBI Behavioral Science Unit has developed and refined the process even further and has been developing

additional classification schemes. In 1990, *Investigative Psychology* (IP) emerged to integrate psychology into criminal and civil investigation through a scientific approach. IP is a sub-discipline of forensic and criminal psychology and explores patterns of criminal behavior to determine a relationship to the offender's characteristics. Hacking is unique in that criminal behavior is not constant, various methods and techniques are used, and hacking is not always associated with a crime. These facts make it challenging to apply a single framework to criminal acts of hacking.

There are sub-fields associated criminal profiling, and with crime opportunity theory such as *routine activity theory* (RAT), *social learning theory* (SLT) and *situational action theory* (SAT). These theories may provide an understanding as to why or how hacking emerges. Opportunity theories of crime seek to explain how crime occurs rather than focusing primarily on criminal disposition. The emphasis is on how opportunity leads to the criminal act, and this theory has received much criticism and subsequent reform.

Marcus Felson and Lawrence Cohen developed RAT, and it focuses upon the situation of the crime. This theory states that crime is "relatively unaffected by social causes such as poverty, inequality or unemployment". This theory is controversial among sociologists who believe in the social causes of crime.

For RAT to occur three things must converge, a motivated offender, a target and the absence of "able guardians". The idea of an able guardian can include security holes, weak security protection or even a lack of appropriate adult guidance or supervision. In some cases, individuals did not receive punishment for hacking systems or hacking attempts may have even been tolerated by authority figures.

The SAT theory was developed in 2004 by Peter Wikstrom and tries to explain moral actions. It attempts to determine why people break the law through unification of sociological, criminological and behavioral science. In this theory, SAT shows that people are moved to action by how they view available options. What they choose depends upon key elements in the situational model. The person and their biological/ psychological make-up and experiences; the setting or environment in which the individual is exposed and reacts to; the situation or perception of the individual of action alternatives and process of choice resulting for his/her interaction with the setting; and the action or bodily movements driven by the individual.

While RAT and SAT help explain the emergence and possible transition of young hackers to adults that hack with criminal intent, these theories are primarily focused upon a lone individual. Earlier I mention that most hackers join a group and at some point evolve from group interaction to other hackers to working alone. While many hack alone to preserve anonymity, at a developmental stage beginning hackers are fostered or sustained socially through mentors or online groups and communities.

Young hackers early attempts at hacking may also be aided through tolerance or reinforcement of their behavior from peers, parents, teachers or administrators. They may join a social network or group that allows them to share or learn a technique, brag about their accomplishments and even form a hacker identity (most have a handle or alias). In this case, SLT offers an additional aid to understanding. Robert Burgess and Ronald Akers developed SLT to explain criminal behavior, and as Akers describes, "social learning is complementary to other sociological theories and could be used to integrate extant formulations to achieve more comprehensive explanations of deviance". In the SLT explanation, a young hacker will engage in criminal behavior as a result of association with others who engage in criminal behavior. This individual will attempt to imitate the actions of others, and is exposed to "definitions (attitudes, norms, and orientations) that justify or rationalize the behavior, and has previously received differential reinforcement rewarding similar behavior". Even reports from the media can add to the glorification and encouragement of criminal hacking behavior.

The actual cause underlying criminal tendency is difficult to determine. However, we have identified a number of motivational themes and situations that lead a young hacker to hack and can lead to criminal activity. These individuals have a deep compulsion to hack, and are driven by curiosity, control, attraction to power and wealth, and even peer recognition or group belonging. Many hackers find offline life boring and only experience a thrill when immersed in the digital world. This can be due to feelings of powerlessness versus the control they feel when hacking or engaging online.

Conclusion

Between 1960 and 2014, evolution occurred in the way hackers use computers, and many hackers have an obsession with technology and computing beyond what lawmakers would consider legal and beyond the code of ethics of hackers from the 50s and 60s. Hackers in the early 50s through the 70s were considered revolutionary and visionaries. They immersed themselves into exploration of technology and computers. They are diverse, creative, and imaginative. They defy expectation and categorization and lead the frontiers of digital exploration.

Individual perspectives on the hacker culture show differing perspectives on community, culture and ethics. However, most articles and books point to a commonality – a common perspective of sharing, openness and improving the world. Much has been written about the various aspects and traits of hackers, but the people I have met and who have taught me in my personal exploration of technology, security and computing have been generous of spirit and creative, freely giving of their wisdom and information.

While there are various theories about how or why young people become hackers, I explain how three theories demonstrate the various evolutionary stages of hacking. RAT explains how an individual starts to hack. SAT explains why an individual would continue to hack even when presented with alternatives, and SLT shows how environment, behavior and culture sustain hacking.

There are other elements that reinforce hacking such as morals, motivation, knowledge and skill. Motivations appear to vary depending upon the individual. Each hacker is different from another due to history, family, and life experiences. These elements are what make a hacker unique but in attempting to identify hacking and hacking behavior there may be a means to provide guidance early to mitigate an individual leaning towards criminal behavior in hacking. It would not be appropriate to attribute characteristics that belong to a few hackers to the group.

There are always individuals who represent an exception although certain characteristics do emerge such as mastery and strong technological skills, fluidity in group membership, secrecy and anonymity. Hackers walk a balance between concealing their hacking activity to avoid gaining the attention of law enforcement and sharing information to gain recognition within the hacker subculture.

I have primarily found articles and research about the individuals who break rules and not the people who create or enforce the rules. I think that a broader perspective and study should include both sides of the equation and the interaction between these groups of people. There is a perception and interpretation that occurs by both parties, and I think the challenge lies in describing perspectives of a singular group as they fail to meet the perspective of the other group. I do not feel that full understanding can come without first understanding and analyzing both the lawmakers and enforcers and the hackers.

With the rapid changes that have occurred over the past forty years in who is considered a hacker and the types of hacks that are encouraged or reinforced, researchers will need to continue to examine the characteristics of the hacker subculture. It is my hope that this information opens up ways to intervene and support young hackers in exploration of computer technology while leading them away from criminal activities.

About the Author

Chrissa Constantine has been working as an Information System Security Engineer and Information Assurance Consultant for the past five years and is also working on a Master of Science from EC-Council University.

UPDATE NOW WITH STIG AUDITING

"IN SOME CASES **nipper studio** HAS VIRTUALLY **REMOVED** the NEED FOR a **MANUAL AUDIT**"

CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at www.titania.com

2012 Computing Security Awards WINNER Enterprise Security Solution of the Year

Security Products' GOVIES 2013 Government Security Awards

2012 Computing Security Awards WINNER Network Security Solution of the Year

www.titania.com